

IAP9 Rec'd PCT/PTO 31 JAN 2006

T03018 PCT

1

Transparent Access Authentication in 2G and 2.5G Mobile
Access Networks

EPO-DG 1

28.04.2005

- 5 The present invention relates to a method and system for
transparent access authentication in 2G and 2.5G Mobile
Access Networks. This includes communication networks of the
GSM-, GPRS- and UMTS-standard well known to skilled persons.
- 10 In standardisation of Universal Mobile Telecommunication
System (UMTS Rel.5) comprehensive means are foreseen to
perform authentication on the application layer with no need
to interwork with the underlying radio and transport
networks. The mechanisms are based on the assumption that a
15 specific environment is prepared for deployment of IP
Multimedia Subsystem (IMS) services. It includes the use of
IMS SIM (ISIM) application, which in turn requires
Rel.99UICC's in the connected end devices to handle the
authentication and key agreement (AKA).
- 20 In case of deployment of IMS and IMS based services in a
network environment which is characterised by the use of SIM
cards, the standardised authentication mechanism will not be
applicable.
- 25 The Technical Specification 3GPP TS 33.203: "Access Security
for IP-based Services", Release 5, V5.6.0, June 2003, XP-
002264085, discloses a method for transparent access
authentication of subscribers connected to an authenticating
network domain by a GPRS core network or an UMTS network, the
30 method using data which are assembled by a network layer
during establishment of a PDP context in GPRS networks.

T03018 PCT

1a.

It is the object of the invention to provide method and system for transparent access authentication which allow it to run authentication transparently to the end device, without requiring proprietary extensions and functions on
5 network or client side.

This object is achieved by providing a method and system as described in the independent claims.

T03018 PCT

10

EPO - DG 1

28.04.2005

26.04.2005

Claims

(82)

1. Method for transparent access authentication of
5 subscribers connected to an authenticating network domain
by a GPRS core network or an UMTS network, wherein the
method using data which are assembled by a network layer
during establishment of a PDP context in GPRS networks,
characterised in
10 that when a Gateway GPRS Support Node (1) receives a
context creation request it queries a registration server
(2) to get an IP address assigned for the particular PDP
context, and within the context the registration server
(2) receives a Mobile Station ISDN Number, MSISDN, and/or
15 an International Mobile Subscriber Identity, IMSI, of the
subscriber and stores for each PDP context a pair of IP
address and IMSI/MSISDN in a session database (3),
that a proxy server (5) is provided which checks
IMSI/MSISDN from a registration server (2) session
20 database (3) and IMSI/MSISDN from a application domain
database (4) for match,
that if the IMSI/MSISDN pairs are matching, the proxy
server (5) checks a subscribers IP address assigned in
the IP network layer for match with the IP address
25 assigned by the registration server (2), and
that the proxy server (5) parses the application layer
for IP addresses given in the headers of registration
messages and checks for match with the network layer IP
address which was already checked for match with the IP
30 address assigned by the radius server (2).
2. Method according to claim 1, comprising the step that
during PDP context establishment a Serving GPRS Support

T03018 PCT

11

Node (SGSN) is authenticating the subscriber using the A3/A8 algorithm based on an end devices SIM card.

3. Method according to any preceding claim, comprising the
5 step that in all subsequent messages arriving at the proxy server (5), it checks for match of IP address in the IP packet overhead field for source address with that in the application layer protocol header fields and verifies the matching pairs against the IP address
10 assigned by the Radius server (2).
4. Method according to any preceding claim, that a routing module (7) is provided which is a standard entry point for all messages and decides by evaluation of Private ID,
15 PrivID, which network node will handle the message.
5. System of units in a mobile telecommunication network, characterised that at least a first authentication unit (2) is connected via a data line to a second unit (5; 6)
20 which assembles data according to the method of claim 1.
6. System according to claim 5, wherein the first unit comprises a registration server (2).
- 25 7. System according to claim 5 or 6, wherein the first unit (2) is connected to a session database (3).
8. System according to any of claims 5 to 7, wherein the second unit comprises a proxy server (5).
- 30 9. System according to any of claims 5 to 8, wherein the second unit comprises a Proxy Call State Control Function (6).

T03018 PCT

12

10. System according to any of claims 5 to 9, wherein the second unit (5; 6) is connected to a subscriber database (4).

5

11. System according to any of claims 5 to 10, wherein a routing module (7) is provided which decides by evaluation of Private ID, PivID, which network node will handle the message.

10